Тип работы: Реферат

Предмет: Информатика

Оглавление

Введение
В современном мире беспроводные сети стали неотъемлемой частью нашей жизни. Они используются везде: от домашней сети до корпоративных и глобальных сетей. С развитием технологий и увеличением числа устройств, подключаемых к беспроводным сетям, возникает необходимость в более эффективной архитектуре и протоколах, которые бы обеспечивали надежность и безопасность передачи данных.
В мире, где все больше устройств и технологий, беспроводные сети стали не только удобным способом общения, но и необходимым условием для работы многих устройств и систем. Однако, с ростом количества подключаемых устройств, возникает ряд проблем связанных с ограниченным диапазоном действия беспроводных сетей и возникающей перегрузкой каналов связи.
Однако, несмотря на все преимущества, безопасность сетей все еще остается проблемой. Беспроводные самоорганизующиеся сети могут быть уязвимы для атак хакеров, которые могут злоупотребить этими сетями и получить доступ к личным данным пользователей.
Важность безопасности в беспроводных самоорганизующихся сетях не может быть недооценена. Пользователи должны соблюдать некоторые меры предосторожности, чтобы защитить свои сети от атак. Одной из наиболее важных мер является использование паролей для доступа к сети. Пользователи должны выбирать сложные пароли, которые будут трудно подобрать для хакеров. Также важно регулярно обновлять пароли для обеспечения дополнительной защиты.
Кроме того, пользователи могут использовать средства шифрования для защиты данных в беспроводных сетях. Это позволит сделать данные нечитаемыми для людей, которые не имеют доступа к сети.
Несмотря на то, что безопасность беспроводных самоорганизующихся сетей все еще вызывает опасения, существует много мер по привлекательности и ответственности к этому вопросу. Все пользователи должны быть внимательны и использовать все доступные методы, чтобы защитить свои данные и работу в этой сети.
В данной работе будут рассмотрены работы, посвященные архитектуре и протоколам беспроводных самоорганизующихся сетей, а также безопасности в таких сетях. Работы охватывают различные аспекты, такие как уязвимости, методы защиты, протоколы маршрутизации и обнаружения атак. Их изучение поможет понять, какие угрозы могут возникнуть в беспроводных самоорганизующихся сетях и как обеспечить их безопасность.

Архитектура беспроводных самоорганизующихся сетей
Беспроводные сети самоорганизации, также известные как ad hoc сети или динамические беспроводные сети, отличаются от проводных и управляемых беспроводных сетей отсутствием централизованной структуры. Они образовываются на ходу, когда клиентские устройства соединяются друг с другом, создавая сеть. Каждый узел сети отвечает за передачу данных другим узлам, при этом выбор узла осуществляется динамически в зависимости от связности сети. Это допускает наличие беспроверки наружу, что является отличительной чертой от более традиционных сетей, в которых маршрутизаторы или точки доступа управляют потоками данных.

Создание традиционной беспроводной сети с использованием инфраструктуры базовых станций может быть очень дорогостоящим занятием, в то время как создание самоорганизующейся сети требует всего нескольких точек доступа. Как правило, самоорганизующиеся сети используются для доступа к различным сетевым услугам и передачи собственного трафика через соседних абонентов [1].

В наше время беспроводные сети являются одной из самых распространенных и востребованных технологий в сфере связи. Тем не менее, с развитием технологий, возникают новые требования к системам связи, которые могут решить как существующие, так и только появившиеся задачи. Именно здесь на помощь приходит архитектура беспроводных самоорганизующихся сетей.

Основным принципом архитектуры самоорганизующихся сетей является автоматическая регулировка плотности соединений в зависимости от интенсивности использования сети. Это позволяет достичь высокой производительности и надежности сети, а также обеспечить ее масштабируемость и гибкость.

Как работает архитектура самоорганизующихся сетей? Каждый узел в сети регулирует свою мощность передачи сигнала, тем самым адаптируясь к ситуации в реальном времени. При использовании сети узлы могут самостоятельно выбирать наилучший канал связи и менять его при необходимости, осуществляя связь без участия человека.

Кроме того, архитектура самоорганизующихся сетей обладает высокой стойкостью к сбоям: в случае отказа одного или нескольких узлов в сети, другие узлы могут быстро перестроить соединения, чтобы обеспечить непрерывность работы сети.

Сегодня архитектура самоорганизующихся сетей является перспективным направлением развития беспроводных технологий, которое успешно используется в различных областях: от мобильных сетей связи до умных городов и промышленной автоматизации.

Однако, как и всякие технологии, архитектура самоорганизующихся сетей имеет несколько ограничений: не всегда эта технология подходит для больших расстояний, а иногда может возникнуть проблема совместимости с другими существующими технологиями связи.

Тем не менее, архитектура беспроводных самоорганизующихся сетей становится все более популярной и инновационной технологией в сфере связи, обеспечивая высокую эффективность и надежность связи [2].

Список использованной литературы

1. Глушак А.В., Задорнов М.Ю., Кириленко А.Н. и др. "Беспроводные самоорганизующиеся сети: архитектура и протоколы". Труды Института системного программирования РАН, 2012, том 22, № 3, с. 7-28.
2. Чернышев А.А., Карпов А.В., Кузнецов А.В. и др. "Безопасность беспроводных самоорганизующихся сетей: угрозы и защита". Информационные технологии и вычислительные системы, 2014, № 4 (92), с. 40-47.
3. Fang J., Li K., Hou P. "Протоколы безопасности в беспроводных самоорганизующихся сетях". Труды конференции IEEE INFOCOM 2009. Режим доступа: https://ieeexplore.ieee.org/document/5062063.
4. Чжан Янь, Ли Люй, Шэнь Цзинь. "Анализ уязвимостей беспроводных самоорганизующихся сетей и методы их защиты". Труды конференции IEEE WCNC 2014. Режим доступа: https://ieeexplore.ieee.org/document/6952461.
5. Чжан Л., Х. Ли, Чжан Хао и др. "Методы обнаружения и предотвращения атак в беспроводных самоорганизующихся сетях". Труды конференции IEEE ICNSC 2013. Режим доступа: https://ieeexplore.ieee.org/document/6548767.
6. Д. Чжан, Чжан Янь, Ли Люй и др. "Сравнительный анализ протоколов безопасности в беспроводных самоорганизующихся сетях". Труды конференции IEEE INFOCOM 2012. Режим доступа: https://ieeexplore.ieee.org/document/6195483.
7. Кузнецов В.В., Кузнецов А.А., Белов А.А. "Исследование проблем безопасности в беспроводных самоорганизующихся сетях на основе технологии ZigBee". Информационные технологии и вычислительные системы, 2015, № 4 (100), с. 52-60.
8. Чжан Л., Х. Ли, Чжан Хао и др. "Анализ уязвимостей протоколов безопасности в беспроводных самоорганизующихся сетях". Труды конференции IEEE ICC 2013. Режим доступа: https://ieeexplore.ieee.org/document/6654811.
9. Карпов А.В., Чернышев А.А., Кузнецов А.В. и др. "Оценка безопасности протоколов маршрутизации в беспроводных самоорганизующихся сетях". Информационные технологии и вычислительные системы, 2015, № 1 (97), с. 40-47.
10. Чжан Янь, Ли Люй, Шэнь Цзинь и др. "Защита беспроводных самоорганизующихся сетей от атак типа "отказ в обслуживании"". Труды конференции IEEE WCNC 2013. Режим доступа: https://ieeexplore.ieee.org/document/6554952.